INFORMATION AND COMPUTATION 77, 233–259 (1988)

# Linear Numeration Systems of Order Two

CHRISTIANE FROUGNY

*LITP et Université René Descartes, U.E.R. de Mathématiques, 12 rue Cujas, 75005 Paris, France*

A numeration system is a sequence of integers such that any integer can be represented by means of the sequence using integers of bounded size. We study numeration systems defined by linear recurrences of order two. We give a necessary and sufficient condition on the system such that every integer has a canonical representation. We show that this canonical representation can be computed from any representation by a rational function. This rational function is the composition of two subsequential functions that are simply obtained from the system. The addition of two integers represented in the system can be performed by a subsequential machine. 

## 1. INTRODUCTION

The way numbers are used is intrinsically related to the way they are represented. The representation of a number is the writing of this number as a word on an alphabet—the alphabet of the digits. The meaning of the word, that is its numerical value, depends on the numeration system considered, like the decimal system, the binary system, the hexadecimal system, etc.

For instance, the process of addition of two numbers depends on their representation. The addition rules are not the same as those say in the binary system and in the decimal system.

Let us give some formal definitions to present our work.

A *numeration system* is given by a strictly increasing sequence of non-negative integers $U=(u_0, u_1, ...)$, called the *basis* of the system, and a finite subset $D$ of $N$, which is the set of *digits*. For every non-negative integer $N$, a *representation* of $N$ in the numeration system $(U, D)$ is a finite sequence $(d_0, ..., d_k)$ of elements of $D$ such that $N = d_0 u_0 + \cdots + d_k u_k$. A representation of $N$ is thus a word $d_0 \cdots d_k$ of the free monoid $D^*$.[1]

Conversely, we define an application $\pi: D^* \to N$ where, if $w = w_0 \cdots w_k$,

[1] I have chosen to write numbers from left to right, like works. For technical reasons, it is convenient to process words and words representing numbers in the same manner. This method, the reverse of the usual one, puts the most significant digit on the right-hand side of the word.



0890-5401/88 $3.00

for $0 \leqslant i \leqslant k$, $w_i \in D$, $\pi(w) = w_0 u_0 + \cdots + w_k u_k$. $\pi(w)$ is the *numerical value* of the word $w$ *in the numeration system* $(U, D)$.

The most used numeration systems are those where $U = (1, k, k^2, ...)$, where $k$ is a non-negative integer, and $D = \{0, 1, ..., k-1\}$, called *k-ary systems*. If we keep the same basis $U$ but take $D = \{1, 2, ..., k\}$ as the set of digits, we obtain *k-adic systems*. More generally, we called *geometrical systems* numeration systems with basis $U = (1, k, k^2, ...)$ and arbitrary finite set $D \subseteq N$. Such systems have been studied by Culik and Salomaa [5] and others [8, 11].

If every integer has a representation in the system $(U, D)$, this system is said to be *complete*, otherwise it is said to be *incomplete*.

The $k$-ary and $k$-adic systems are complete. Moreover, in a $k$-ary system, every positive integer has a unique representation which satisfies the condition that the digit of greatest pound is not 0. In a $k$-adic system, every positive integer has a unique representation.

The uniqueness of representation is far from being a general rule. For instance, in geometrical systems with arbitrary set $D$, there can be more than one representation (cf. [5]). Systems in which an integer can have several representations are called *ambiguous* systems. If the representation of every integer is unique, the system is said to be *unambiguous*.

A less classical example of a numeration system is the *Fibonacci numeration system*. Let $F = (1, 2, 3, 5, 8, ...)$ be the sequence of Fibonacci numbers defined by

$$f_{n+2} = f_{n+1} + f_n$$
$$f_0 = 1, \qquad f_1 = 2.$$

It is known that, with $D = \{0, 1\}$, $(F, D)$ is a complete numeration system (cf. Zeckendorf [13], Carlitz [3], and Knuth [10]). In the Fibonacci numeration system an integer may have several representations.

EXAMPLE 1. Fibonacci numeration system,

| $F=$ | 1 | 2 | 3 | 5 | 8 | 13 | 21 | $\cdots$ |
|---|---|---|---|---|---|---|---|---|
| $24=$ | 1 | 1 | 1 | 1 | 0 | 1 | | |
| $=$ | 1 | 1 | 0 | 0 | 1 | 1 | | |
| $=$ | 0 | 0 | 1 | 0 | 1 | 1 | | |
| $=$ | 1 | 1 | 0 | 0 | 0 | 0 | 1 | |
| $=$ | 0 | 0 | 1 | 0 | 0 | 0 | 1. | |

However, in $(F, \{0, 1\})$, every integer has a unique representation which does not contain two consecutive digits equal to 1 and has no 0 to its right-hand side (Zeckendorf [13]). In Example 1, the representation of 24 which satisfies this condition is the last one, 0010001.

The problem of determining the conditions under which the representation of integers in a given numeration system is unique has been discussed in particular by Fraenkel [7].

Our point of view is the following. In numeration systems which may be ambiguous, we define a canonical representation (analogous to that of Zeckendorf in the Fibonacci system) and we study the nature of the function which to any representation associates the canonical representation. We focus on numeration systems, the basis of which is defined by a linear recurrence equation. Such systems are called *linear numeration systems.* We prove that, under certain conditions, every integer has a canonical representation in a linear numeration system. The function which associates the canonical representation of an integer to any representation of that integer can be shown to be "simple." More precisely, it is a rational function, i.e., a function which can be computed by a finite state machine.

In order to be more precise, we need several definitions: given a numeration system $(U, D)$ we define two equivalence relations on $D^*$.

First we say that two words are *numerically equivalent* if they have the same numerical value. More formally,

DEFINITION. The *numerical equivalence* $\pi$ associated to the system $(U, D)$ is defined by

$$\forall f, g \in D^*, \qquad f \sim_\pi g \Leftrightarrow \pi(f) = \pi(g).$$

It is clear that, in the general case, $\pi$ is not a congruence.

We now consider numerically equivalent words which have the same length. That leads to the following:

DEFINITION. The *alphanumerical equivalence* $\alpha$ associated to the system $(U, D)$ is defined by

$$\forall f, g \in D^*, \quad f \sim_\alpha g \Leftrightarrow \begin{cases} \pi(f) = \pi(g) \\ |f| = |g|, \end{cases}$$

where $|f|$ denotes the length of the word $f$.

Let $f$ and $g$ be two words of same length of $D^*$. We shall say that $f$ is *greater* than $g$, denoted by $f \succ g$, if the reverse image $\tilde{f}$ of $f$ is greater than $\tilde{g}$ for the lexicographical ordering. (This ordering is the same as the usual numerical ordering in $k$-ary systems.)

EXAMPLE 1 (continued). The word 0010001 is greater than the word 1100001.

Let $f$ be a word of $D^*$. In the equivalence class of $f$ modulo $\alpha$, we choose the greatest word—denoted by $\bar{f}$—for the ordering $\succ$ defined supra. This word $\bar{f}$ is called the *normal form* of $f$. We shall say that $\bar{f}$ is the *canonical representation* of the integer $\pi(f)$ in the system $(U, D)$. The function $\nu$: $f \in D^* \to \bar{f} \in D^*$ is called the *normalization* associated to $(U, D)$.

EXAMPLE 1 (continued). The normal form of the word 1100001 is the word 0010001, which is the canonical representation in the Fibonacci system of the integer 24. The notion of canonical representation here is the same as the Zeckendorf representation.

In this paper, we consider the sequence $U$ defined by the linear recurrence relation of order two,

$$u_{n+2} = au_{n+1} + bu_n$$
$$u_0 = 1, \qquad u_1 = u \geqslant 2,$$

where $a$ and $b$ are two integers $\geqslant 1$ (the Fibonacci case is thus a particular case with $a = b = 1$ and $u = 2$). As a set of digits we take $D = \{0, 1, ..., s\}$ where $s$ is an integer $>0$. We write $[s]$ instead of $D$, and $(U_u, s)$ instead of $(U, D)$, since the system depends on two parameters, the greatest digit $s$ and the initial value $u$.

We show that there exists only one value of $u$ and $s$, namely $u = a + 1$ and $s = a$, for which the linear numeration system $(U_u, s)$ is complete and the associated alphanumerical equivalence is a cancellative congruence (Theorem 1). For these values of $u$ and $s$ we give a series of results. The alphanumerical equivalence associated to the numeration system $(U_{a+1}, a)$ can be shown to be equal to the congruence generated by the Thue-system $R_a$ directly derived from the linear recurrence relation defining the basis $U_{a+1}$ (Theorem 2). The system $R_a$ induces a rewriting system, which is confluent and noetherian and thus we define a reduction function. We show that the normal form of a word in the system $(U_{a+1}, a)$ is the image of this word by the reduction function (Proposition 10). We then prove that this reduction can be obtained as the composition of two subsequential machines, one processing words from left to right and the other from right to left (Theorem 3). Thus the normalization is a rational function.

It is known that the process of addition of two integers represented in the $k$-ary system can be performed by a left-subsequential machine [6, 1]. Berstel [2] has shown that in the Fibonacci numeration system, the addition can be realized by a right-subsequential machine. We show that this is still true in the system $(U_{a+1}, a)$. More precisely, we use the following method. Taking any representations of two integers, we add them digit by digit. The resulting word belongs then to the set $[2a]^*$. It can be shown (Theorem 4) that an equivalent word belonging to $[a]^*$ can be computed by means of a right-subsequential function, which is a kind of a partial normalization. The addition in $k$-ary systems is left-subsequential, while it is right-subsequential in the linear system. This could be explained as follows. The transformation from $[2a]^*$ onto $[a]^*$ in the linear case does not give a result in normal form, and thus the normalization—which is not subsequential—should be applied again.

As a last consequence of Theorem 4 we get that, if we take a finite arbitrary set of digits $D$ instead of $\{0, ..., a\}$, it is possible to reduce the system $(U_{a+1}, D)$ to the perfect system $(U_{a+1}, a)$ with a right-subsequential function.

## 2. Completeness

The sequence $U$ being defined by the linear recurrence relation

$$u_{n+2} = au_{n+1} + bu_n, \qquad a, b \text{ fixed integers} \geqslant 1,$$

with initial values $u_0 = 1$ and $u_1 = u \geqslant 2$, we shall denote it by $U_u$. The set of digits $D$ is $\{0, 1, ..., s\}$ and is denoted by $[s]$.

Our aim is to determine the values of the parameters $u$ and $s$ for which the system is complete.

We need the following lemmas.

LEMMA 1. *For every integer* $i \geqslant 0, j \geqslant 1$, *we have* $au_i + au_{i+1} + \cdots + au_{i+j} = -bu_{i-1} - bu_i + (1-b)u_{i+1} + \cdots + (1-b)u_{i+j-1} + u_{i+j} + u_{i+j+1}$, *with convention that* $bu_{-1} = u_1 - au_0$.

*Proof.* It follows easily from the fact that, for $0 \leqslant k \leqslant i+j$, $au_k = u_{k+1} - bu_{k-1}$. ∎

LEMMA 2. *Any system* $(U, s)$ *is complete if and only if* $s(u_0 + \cdots u_k) \geqslant u_{k+1} - 1$ *for every* $k \geqslant 0$.

*Proof.* If $s(u_0 + \cdots + u_k) < u_{k+1} - 1$, the system $(U, s)$ is incomplete because $u_{k+1} - 1$ has no representation. Assume that $s(u_0 + \cdots + u_k) \geqslant u_{k+1} - 1$ for every $k \geqslant 0$. Let $N$ be a positive integer such that any integer smaller than $N$ is representable, and let $m$ such that $u_m \leqslant N < u_{m+1}$. Choose $t$ such that $tu_m \leqslant N < (t+1)u_m$. We take $r = t$ if $t < s$ and $r = s$ if $t \geqslant s$. We claim that

(1) $N - ru_m \geqslant 0$

(2) $N - ru_m \leqslant s(u_0 + \cdots + u_{m-1})$.

If $r = t < s$, (1) is valid. $N < (r+1)u_m$; hence $N - ru_m \leqslant u_m - 1 \leqslant s(u_0 + \cdots + u_{m-1})$.

If $r = s \leqslant t$, $ru_m \leqslant tu_m \leqslant N$ and (1) is valid. Now, $N - ru_m = N - su_m \leqslant s(u_0 + \cdots + u_{m-1})$. Otherwise $N > s(u_0 + \cdots + u_m) \geqslant u_{m+1} - 1$ which is impossible.

The conditions (1) and (2) and the induction hypothesis imply that $N - ru_m$ is representable by a word $w$ of length $m$, and $N$ is representable by the word $wr$. ∎

We now have

PROPOSITION 1. *If $s \leqslant u-2$ or $s \leqslant a-1$, the numeration system $(U_u, s)$ is incomplete.*

*Proof.* First, if $s \leqslant u-2$ then at last the integer $u-1$ has no representation. Second, if $s \leqslant a-1$ then there exists an index $i$ such that $S = su_0 + \cdots + su_i < u_{i+1} - 1$. Since $s \leqslant a-1$, $S \leqslant (a-1)(u_0 + \cdots + u_i)$, and, by Lemma 1, $S \leqslant a - 1 - b - (b+1)u_1 - bu_2 \cdots - bu_{i-1} + u_{i+1}$. So, $S < u_{i+1} - 1$ if $a < b + (b+1)u_1 + bu_2 + \cdots + bu_{i-1}$, which is necessarily true for one $i$. ∎

PROPOSITION 2. *Suppose $a \leqslant b-2$. If $s = a$ then the system $(U_u, s)$ is incomplete.*

*Proof.* The integer $u_2 - 1$ cannot be represented, for $su_0 + su_1 = a + au_1 < u_2 - 1 = au_1 + b - 1$. ∎

PROPOSITION 3. *If $a \geqslant b-1$, $s \geqslant a$, and $s \geqslant u-1$, the system $(U_u, s)$ is complete.*

*Proof.* We show that $s(u_0 + \cdots + u_k) \geqslant u_{k+1} - 1$ for every $k \geqslant 0$. If $k = 0$, we have $s \geqslant u-1$ by assumption. Suppose inductively that $s(u_0 + \cdots + u_k) \geqslant u_{k+1} - 1$. Then $s(u_0 + \cdots + u_{k+1}) \geqslant u_k - 1 + su_k + su_{k+1} \geqslant u_k - 1 + (b-1)u_k + au_{k+1} = u_{k+2} - 1$. ∎

REMARK 1. *For $a \leqslant b-2$, $s \geqslant a+1$, and $s \geqslant u-1$, the system $(U_u, s)$ can be either complete or incomplete.*

If we take $s = a+1$ and $u = a+2$, when $b > 2(a+2)$ the integer $u_2 - 1$ cannot be represented.

EXAMPLE 2. $a = 1$, $b = 6$, $u = 3$, $s = 2$ gives a complete system. $a = 1$, $b = 7$, $u = 3$, $s = 2$ gives an incomplete system. (9 has no representation in it.)

## 3. Alphanumerical Equivalence

We study how the properties of the alphanumerical equivalence $\alpha$ associated to the system $(U_u, s)$ depend on the parameters $u$ and $s$.

By definition of $\alpha$, it is possible to replace a factor of a representation of an integer by a factor of the same length and having the same numerical value.

We say that a numeration system is *regular* if its associated alphanumerical equivalence $\alpha$ is a congruence. If $\alpha$ is a cancellative equivalence, we say that the system is *cancellative*. A numeration system is said to be *perfect* if it is a complete, regular, and cancellative numeration system. This condition of perfection is a natural one when working on the representation of integers, since it means (1) that every integer has a representation (completeness); (2) that if $f$ and $g$ are two words representing the same integer, and $h$ any word, $fh$ and $gh$ represent the same integer, and $hf$ and $hg$ represent the same integer (regularity); (3) and that if $fh$ and $gh$ (or $hf$ and $hg$) represent the same integer, then $f$ and $g$ represent the same integer (cancellativity).

Our aim is to prove the following.

THEOREM 1. *If $a \geqslant b$, the numeration system $(U_u, s)$ is perfect if and only if $s = a$ and $u = a + 1$.*

We introduce a notation: if $f = f_0 \cdots f_k$, with $f_i \in D$, we denote by $\pi_j(f) = f_0 u_j + f_1 u_{j+1} + \cdots + f_k u_{j+k}$, for $j \geqslant 0$. So $\pi(f) = \pi_0(f)$. We then have, for a word $h \in D^*$, $\pi(fh) = \pi(f) + \pi_{|f|}(h)$.

DEFINITIONS. The equivalence $\beta$ is said to be *left-* (resp. *right*)*-regular* if the following holds: $\forall f, g, h$, $f \sim_\beta g$ implies $hf \sim_\beta hg$ (resp. $fh \sim_\beta gh$). If it is both left- and right-regular, it is *regular*. The equivalence $\beta$ is said to be *left-* (resp. *right*)*-cancellative* if $\forall f, g, h$, $hf \sim_\beta hg$ (resp. $fh \sim_\beta gh$) implies $f \sim_\beta g$. If it is both left- and right-cancellative then it is *cancellative*.

It is easy to see that in the case of the alphanumerical equivalence $\alpha$, we have the following.

PROPOSITION 4. *The alphanumerical equivalence $\alpha$ associated to any numeration system $(U, D)$ is right-cancellative and right-regular.*

*Proof.* Let $f$, $g$, and $h$ be words of $D^*$. We have $f \sim_\alpha g$ iff $\pi(f) = \pi(g)$ and $|f| = |g|$. Thus $f \sim_\alpha g \Leftrightarrow fh \sim_\alpha gh$, since $\pi(fh) = \pi(f) + \pi_{|f|}(h)$ and $\pi(gh) = \pi(g) + \pi_{|g|}(h)$. ∎

For the left side we have that the alphanumerical equivalence $\alpha$ is left-regular if and only if the following holds: $\forall i, k \geqslant 0$, $\forall f, g \in D^*$, $\pi_k(f) =$

$\pi_k(g) \Rightarrow \pi_{i+k}(f) = \pi_{i+k}(g)$. $\alpha$ is left-cancellative if and only if the converse is true, that is $\pi_{i+k}(f) = \pi_{i+k}(g) \Rightarrow \pi_k(f) = \pi_k(g)$.

The recurrence relation $u_{n+2} = au_{n+1} + bu_n$ implies that the words 001 and $ba0$ are alphanumerically equivalent, and, more generally that, for every $k \geqslant 0$, $0^k001$ and $0^kba0$ are alphanumerically equivalent, that is $\pi_k(001) = \pi_k(ba0)$.

Under certain conditions on the system, we shall see that the same property holds for every pair of words $f$, $g$ such that $f \sim_\alpha g$, and then that $\alpha$ is left-regular.

EXAMPLE 3.

$$u_{n+2} = 2u_{n+1} + u_n$$

$$u_0 = 1, \qquad u_1 = 3, \qquad s = 2$$

$U = \{1, 3, 7, 17, 41, 99, 239, 577 \ldots\}$

| | 1 | 3 | 7 | 17 | 41 | 99 | 239 | 577 | $\cdots$ |
|---|---|---|---|---|---|---|---|---|---|
| (1) | | | 1 | 2 | 1 | 2 | 1 | | |
| | | | 0 | 0 | 1 | 0 | 2 | | |
| (2) | | 1 | 2 | 1 | 2 | 1 | | | |
| | | 0 | 0 | 1 | 0 | 2 | | | |
| (3) | | | | 1 | 2 | 1 | 2 | 1 | |
| | | | | 0 | 0 | 1 | 0 | 2 | |

Let $f = 12121$ and $g = 00102$.

We have $\pi_2(f) = \pi_2(g) = 519$ (1). It can be verified that $\pi_1(f) = \pi_1(g)$ (2) and $\pi_0(f) = \pi_0(g)$, and that, for $i \geqslant 3$, $\pi_i(f) = \pi_i(g)$. These are consequences of the fact that $\alpha$ is left-cancellative and left-regular as we shall prove infra (Propositions 7 and 8).

We describe now the properties of the alphanumerical equivalence $\alpha$ associated to the system $(U_u, s)$ according to the values of $u$ and $s$.

LEMMA 3. *Let $P(x) = x^2 - ax - b$ be the characteristic polynomial associated to the linear recurrence $u_{n+2} = au_{n+1} + bu_n$. If $a \geqslant b$ then $P$ has no positive integer root. If $a < b$ then $P$ has a positive integer root, equal to $a + i$, where $i$ is an integer $\geqslant 1$, if and only if $b = i(a+i)$.*

*Proof.* We have $P(a) < 0$ and $P(a+1) = a - b + 1$. Hence if $a \geqslant b$, $P(a+1) > 0$, and $P$ cannot have a positive integer root. It is straightforward to verify that the positive root $x = (a + \sqrt{a^2 + 4b})/2$ is equal to $a + i$, for some $i \geqslant 1$, if and only if $b = i(a+i)$. ∎

We now show that, when $u$ is a root of $P$, the corresponding numeration system is degenerate; that is the linear recurrence is no longer of order two.

PROPOSITION 5. *If $u$ is a root of the characteristic polynomial $P$, then the system $(U_u, s)$ reduces to a geometrical system of basis $U = \{(a+i)^k \mid k \geq 0\}$ for an integer $i \geq 1$.*

*Proof.* From Lemma 3 we know that if $P(u)=0$ then $u=a+i$ and $b=i(a+i)$ for some $i \geq 1$. We have $u_2=(a+i)^2$ and, for every $k \geq 0$, $u_k=(a+i)^k$. Hence $(U_u, s)$ is a geometrical system of basis $\{(a+i)^k \mid k \geq 0\}$. ∎

COROLLARY 1. *If $u=a+i$, $i \geq 1$, is a root of $P$, the geometrical system obtained is cancellative and regular. It is complete if and only if $s \geq a+i-1$.*

*Proof.* Since the basis of the system is a geometrical sequence, the alphanumerical equivalence $\alpha$ is left-cancellative and left-regular; hence the system is cancellative and regular, for every $s$.

If $s<a+i-1$, the system is incomplete (because $a+i-1$ has no representation).

If $s=a+i-1$, then the system becomes the classical $(a+i)$-ary system, with basis $\{(a+i)^k \mid k \geq 0\}$ and digits $\{0, 1, ..., a+i-1\}$, and thus is complete and unambiguous, with the condition that the digit of greatest pound is not 0.

If $s>a+1-1$, the system is complete and ambiguous. ∎

We now turn to the non-degenerate case, that is the case where $u$ is not a root of the characteristic polynomial $P$.

We have

REMARK 2. *Suppose $u$ is not a root of $P$. If $s \geq u$, $\alpha$ is not left-regular.*

*Proof.* Consider $v=u0$ and $w=01$. $\pi(v)=\pi(w)$, but $\pi_1(v) \neq \pi_1(w)$; hence $\alpha$ is not left-regular. ∎

REMARK 3. *Suppose $u$ is not a root of $P$. If $s \geq a+1$, the system $(U_u, s)$ is incomplete or non-regular.*

*Proof.* By Remark 2, we may suppose that $s<u$. From Proposition 1, if $s \leq u-2$ the system is incomplete. We suppose then that $s=u-1$.

(1) Suppose $a \geq b-2$. Since $s \geq a+1$, we have $u \geq a+2 \geq b$. The two words $y=0(a+1)0$ and $z=(u-b)01$ of $[s]^*$ are such that $\pi(y)=\pi(z)$ and $\pi_1(y) \neq \pi_1(z)$. Then $\alpha$ is not left-regular.

(2) Suppose now $a \leqslant b-3$.

(a) If $u \geqslant b$, as above $\alpha$ is not left-regular.

(b) If $u \leqslant b-1$, we have two cases to consider. If $b-u \leqslant s=u-1$, the two words $x=001$ and $t=(b-u)(a+1)0$ have same value but $\pi_1(x) \neq \pi_1(t)$. Thus $\alpha$ is not left-regular.

If $b-u>s$, then $b \geqslant 2u$, and we have again two cases.

($\alpha$) $s=a+1$. Then $u=a+2$. Since $u$ is not a root of $P$, $b$ cannot be equal to $2u$ (Lemma 3), and thus $b>2u$. It is easy to verify that $u_2=au+b>u^2$; hence the integer $u_2-1$ has no representation in the system. Thus the system is incomplete.

($\beta$) $s \geqslant a+2$. We have $\pi(001)=\pi((b-2u)(a+2)0)$ if $b-2u \leqslant s$, i.e., $b \leqslant 3u-1$. In that case $\alpha$ is not left-regular.

As above, if $b \geqslant 3u$ we can prove that if $s=a+2$ the system is incomplete and if $s \geqslant a+3$, $\pi(001)=\pi((b-3u)(a+3)0)$ and $\alpha$ is not left-regular if $b \leqslant 4u-1$, and so on. ∎

We now consider the case $a<b$.

PROPOSITION 6. *Suppose $u$ is not a root of $P$, and $a<b$. The numeration system $(U_u, s)$ is incomplete or non-regular.*

*Proof.* Suppose $a \leqslant b-2$. If $s \leqslant a$, the system is incomplete by Propositions 1 and 2. If $s \geqslant a+1$, it is non-regular by Remark 3.

Suppose now $a=b-1$. By hypothesis, $u$ is not a root of $P$, so $u$ is not equal to $a+1$ (Lemma 3). If $s \geqslant a+1$, $\alpha$ is not left-regular or the system is incomplete (Remark 3). If $s \leqslant a-1$, the system is incomplete (Proposition 1). If $s=a$ and $u \leqslant a$, $\alpha$ is not left-regular by Remark 2. If $s=a$ and $u \geqslant a+2$, the system is incomplete by Proposition 1. ∎

Then, a system defined by the relation $u_{n+2}=au_{n+1}+bu_n$, where $b>a$, is either non-perfect or a geometrical system.

Until the end of this paper, we shall consider only the case where $a \geqslant b$, when the system is really of order two.

In order to prove Theorem 1, we need technical results.

PROPOSITION 7. *Let $f$ and $g$ be two words of $[a]^*$ such that $\pi_i(f)=\pi_i(g)$ for an integer $i$ greater than 0. Then $\pi_{i-1}(f)=\pi_{i-1}(g)$.*

The proof uses certain lemmas.

LEMMA 4. *For every* $i \geqslant 0$, $k \geqslant 0$,

$$\pi_i(a^k) \leqslant -bu_{i-1} - bu_i + u_{i+k-1} + u_{i+k}.$$

*Moreover, if* $i=0$ *and* $u > a-b$, *or if* $i \geqslant 1$, $\pi_i(a^k) < u_{i+k-1} + u_{i+k}$.

*Proof.* The first inequality is a mere consequence of Lemma 1. If $i=0$ and $u > a-b$, or $i \geqslant 1$, $-bu_{i-1} - bu_i$ is always negative. ∎

LEMMA 5. *Let* $f = f_0 \cdots f_k$ *and* $g = g_0 \cdots g_k$ *be two words of* $[a]^*$ *of length* $k+1$, $k$ *greater than one. We suppose that* $f_k$ *is greater than* $g_k$ *and that there exists an integer* $i$ *for which* $\pi_i(f) = \pi_i(g)$. *If this integer* $i$ *is greater than* 0, *or if* $u$ *is greater than* $a-b$, *then* $g_k = f_k - 1$ *and* $g_{k-1} = a$. *Moreover if* $f_k = 1$ *then* $f_{k-1} = 0$.

*Proof.* We suppose that $p = f_k - g_k$. Since $\pi_i(f) = \pi_i(g)$, we obtain $\pi_i(f_0 \cdots f_{k-1} p) = \pi_i(g_0 \cdots g_{k-1} 0) \leqslant \pi_i(a^k) < u_{i+k-1} + u_{i+k}$ from Lemma 4.

From $\pi_i(f_0 \cdots f_{k-1} p) < u_{i+k-1} + u_{i+k}$, we deduce, if $p \geqslant 2$, that $f_0 u_i + \cdots + f_{k-1} u_{i+k-1} + (p-1) u_{i+k} - u_{i+k-1} < 0$, which is impossible since $(p-1) u_{i+k} - u_{i+k-1}$ is $>0$. Then $p$ is equal to 1 and $g_k = f_k - 1$.

Now, suppose that $g_{k-1} \leqslant a-1$. We obtain $\pi_i(f_0 \cdots f_{k-1} 1) \leqslant \pi_i(g_0 \cdots g_{k-2}(a-1)0) \leqslant \pi_i(a^{k-1}) + (a-1) u_{i+k-1} < u_{i+k-2} + u_{i+k-1} + (a-1) u_{i+k-1} = u_{i+k-2} + a u_{i+k-1}$.

We then have $\pi_i(f_0 \cdots f_{k-1}) < u_{i+k-2} + a u_{i+k-1} - u_{i+k} = (1-b) u_{i+k-2} \leqslant 0$, which is impossible. Thus $g_{k-1}$ is equal to $a$.

Suppose now that $f_k = 1$ and $f_{k-1}$ is $\geqslant 1$, i.e., $f_{k-1} = 1 + h$ where $h \geqslant 0$. We have $\pi_i(f_0 \cdots f_{k-2}(1+h)1) = \pi_i(g_0 \cdots g_{k-2} a 0)$; thus $\pi_i(f_0 \cdots f_{k-3}(f_{k-2}+b)(1+h)) = \pi_i(g_0 \cdots g_{k-2}) \leqslant \pi_i(a^{k-1}) < u_{i+k-2} + u_{i+k-1}$ (Lemma 4). From that, we deduce that $\pi_i(f_0 \cdots f_{k-3}(f_{k-2}+b-1)h) < 0$, which is not possible. So $f_{k-1} = 0$. ∎

LEMMA 6. *Under the assumptions of Lemma* 5 *with* $k$ *greater than* 2, *we have: if* $f_k = 1$ *and* $f_{k-2} = a-b+h$, *where* $0 < h \leqslant b$, *then* $h=1$ *and* $g_{k-2} = a$.

*Proof.* From $\pi_i(f) = \pi_i(g)$ we deduce that $\pi_i(f_0 \cdots f_{k-3}(a+h)) = \pi_i(g_0 \cdots g_{k-2}) \leqslant \pi_i(a^{k-1})$, so $\pi_i(f_0 \cdots f_{k-3} h) \leqslant \pi_i(a^{k-2}) < u_{i+k-3} + u_{i+k-2}$ (Lemma 4). Suppose that $h = 1 + h'$, with $h' > 0$. Then $\pi_i(f_0 \cdots f_{k-3} h') < u_{i+k-3}$, so $\pi_i(f_0 \cdots f_{k-3}) + h' b u_{i+k-4} + h'(a-1) u_{i+k-3} < 0$, which is not possible. Thus $h=1$.

Now suppose that $g_{k-2} \leqslant a-1$. We obtain $\pi_i(f_0 \cdots f_{k-3} 2) \leqslant \pi_i(g_0 \cdots g_{k-3}) \leqslant \pi_i(a^{k-2}) < u_{i+k-3} + u_{i+k-2}$; thus $\pi_i(f_0 \cdots f_{k-3} 1) < u_{i+k-3}$ which is impossible since $\pi_i(f_0 \cdots f_{k-3} 1) = \pi_i(f_0 \cdots f_{k-3}) + u_{i+k-2}$. Hence $g_{k-2} = a$. ∎

We now prove Proposition 7:

*Proof.* The proof is by induction on $N=\pi_i(f)$. If $N=0$, the result is trivial. Let us suppose the property stated above is verified for every integer $<N$. Let $f=f_0\cdots f_k$ and $g=g_0\cdots g_k$, $f_i$, $g_i\in[a]$.

(1) Suppose that $f_k=g_k$ $(\neq 0)$. Then $\pi_i(f_0\cdots f_{k-1})=\pi_i(g_0\cdots g_{k-1})<N$ and the result is obtained by applying the induction hypothesis.

(2) Suppose that $f_k>g_k$. We know, by Lemma 5, that $g_k=f_k-1$ and $g_{k-1}=a$. From $\pi_i(f)=\pi_i(g)$ we deduce that

$$\pi_i(f_0\cdots f_{k-1}1)=\pi_i(g_0\cdots g_{k-2}a0).$$

(a) If $f_k>1$, $\pi_i(f_0\cdots f_{k-1}1)<\pi_i(f)$; we can thus apply the induction hypothesis, that is $\pi_{i-1}(f_0\cdots f_{k-1}1)=\pi_{i-1}(g_0\cdots g_{k-2}a0)$. So we have $\pi_{i-1}(f_0\cdots f_{k-1}1)+g_ku_{i+k}=\pi_{i-1}(g_0\cdots g_{k-2}ag_k)$, i.e., $\pi_{i-1}(f)=\pi_{i-1}(g)$.

(b) If $f_k=1$, $g_k=0$, $g_{k-1}=a$, and $f_{k-1}=0$ (by lemma 5). We thus obtain $\pi_i(f_0\cdots f_{k-2}01)=\pi_i(g_0\cdots g_{k-2}a0)$.

There are two cases to consider:

($\alpha$) $f_{k-2}\leqslant a-b$. Then $\pi_i(f_0\cdots f_{k-2}01)=\pi_i(f_0\cdots(f_{k-2}+b)\,a0)$ and $\pi_i(f_0\cdots(f_{k-2}+b))=\pi_i(g_0\cdots g_{k-2})<N$. By induction hypothesis, $\pi_{i-1}(f_0\cdots(f_{k-2}+b))=\pi_{i-1}(g_0\cdots g_{k-2})$, and thus $\pi_{i-1}(f)=\pi_{i-1}(f_0\cdots(f_{k-2}+b)\,a0)=\pi_{i-1}(g_0\cdots g_{k-2}a0)=\pi_{i-1}(g)$.

($\beta$) $f_{k-2}>a-b$. By Lemma 6, we know that $f_{k-2}=a-b+1$ and $g_{k-2}=a$. $\pi_i(f)=\pi_i(g)$ implies $\pi_i(f_0\cdots f_{k-3}1)=\pi_i(g_0\cdots g_{k-3}0)<N$; hence $\pi_{i-1}(f_0\cdots f_{k-3}1)=\pi_{i-1}(g_0\cdots g_{k-3}0)$ and thus $\pi_i(f)=\pi_i(g)$. ∎

We now have a kind of converse of that result.

PROPOSITION 8. *Let $f$ and $g$ be two words of $[a]^*$ such that $\pi_i(f)=\pi_i(g)$ for an integer i. If i is greater than* 0, *or if u is greater than or equal to* $a+1$, *then* $\pi_{i+1}(f)=\pi_{i+1}(g)$.

*Proof.* The proof is similar to that of Proposition 7, by using Lemmas 5 and 6 (if $u\geqslant a+1$ then $u>a-b$). ∎

*Remark.* Why this condition $u\geqslant a+1$ when $i\geqslant 0$? This is due to Remark 2, which states that if $u\leqslant s$ then $\alpha$ is not left-regular. Since $s=a$, we obtain that $u$ should be $\geqslant a+1$.

*Proof of Theorem* 1. Recall that, from Propositions 5 and 6, we consider only the case where $a\geqslant b$, and so $u$ is not a root of the characteristic polynomial.

(1) If $s=a$ and $u=a+1$, the numeration system is complete, from Proposition 3. By Proposition 7 the alphanumerical equivalence $\alpha$ is left-cancellative, and by Proposition 8 $\alpha$ is left-regular. Since $\alpha$ is right-cancellative and right-regular (Proposition 4), the numeration system $(U_{a+1}, a)$ is perfect.

(2) • If $s \leqslant a-1$, the numeration system is incomplete (Proposition 1).

• If $s=a$ and $u \geqslant a+2$, the system is incomplete (Proposition 1).

• If $s=a$ and $u \leqslant a$, the alphanumerical equivalence $\alpha$ is not left-regular (Remark 2).

• If $s \geqslant a+1$ then $\alpha$ is not left-regular (cf. Remark 3). ∎

## 4. Congruence Associated to a Linear Numeration System

We have already mentioned that the recurrence relation $u_{n+2} = au_{n+1} + bu_n$ implies that the words ba0 and 001 are alphanumerically equivalent. By addition, we obtain that for every $b \leqslant h \leqslant s$, $0 \leqslant k \leqslant s-1$, $0 \leqslant j \leqslant s-a$, the words $h(a+j)k$ and $(h-b)\,j(k+1)$ are alphanumerically equivalent.

To the system $(U_u, s)$, with $s \geqslant a$, we associate the congruence on $[s]^*$ generated by $R_s = \{(h(a+j)k,\ (h-b)\,j(k+1)) \mid b \leqslant h \leqslant s,\ 0 \leqslant k \leqslant s-1,\ 0 \leqslant j \leqslant s-a\}$.

Theorem 2. *If $u=a+1$ and $s=a$, the alphanumerical equivalence $\alpha$ associated to the system $(U_{a+1}, a)$ is equal to the congruence on $[a]^*$ generated by $R_a$.*

The proof of Theorem 2 is similar to the proof of Proposition 8. This is not surprising since Theorem 2 implies that the alphanumerical equivalence $\alpha$ is left-regular in the particular case where $s=a+1$ and $u=a$ (compare with Proposition 8).

*Proof.* It is obvious that if two words are congruent mod $R_a$, they are congruent mod $\alpha$. For the converse, we need the following lemma.

Lemma 7. *Let $f=f_0 \cdots f_k$ and $g=g_0 \cdots g_k$ be two words of $[a]^*$ such that $f \sim_{R_a} g$. Then for every $0 \leqslant i \leqslant k$,*

$$f_0 \cdots f_{i-1}(f_i+p)f_{i+1} \cdots f_k \sim_{R_a} g_0 \cdots g_{i-1}(g_i+p)\,g_{i+1} \cdots g_k$$

*for every $p$ such that $f_i+p$ and $g_i+p \in [a]$.*

*Proof.* Let us denote by $\hat{p}_i$ the word $0^i p 0^{k-i}$. If $h = h_0 \cdots h_k$ and $h' = h'_0 \cdots h'_k$, we define $h + h'$ as the word $(h_0 + h'_0) \cdots (h_k + h'_k)$. With those notations, we must prove that $f \sim_{R_a} g$ implies $f + \hat{p}_i \sim_{R_a} g + \hat{p}_i$, if $f + \hat{p}_i$ and $g + \hat{p}_i \in [a]^*$.

First, if $(v, w) \in R_a$, it is clear that $v + \hat{p}_i \sim_{R_a} w + \hat{p}_i$. So if $f = xvz$ and $g = xwz$ with $(v, w) \in R_a$, then $f + \hat{p}_i \sim_{R_a} g + \hat{p}_i$.

Now, suppose that $f = w_0 \sim_{R_a} w_1 \cdots \sim_{R_a} w_n = g$, where for every $0 \leqslant j \leqslant n-1$, $w_j = x_j u_j z_j$, $w_{j+1} = x_j v_j z_j$, and $(u_j, v_j) \in R_a$.

By induction, $f + \hat{p}_i \sim_{R_a} w_{n-1} + \hat{p}_i$ and $w_{n-1} + \hat{p}_i \sim_{R_a} g + \hat{p}_i$. ∎

Let $f$ and $g$ be two words of $[a]^*$ such that $f \sim_\alpha g$, i.e., $\pi(f) = \pi(g) = N$. The proof is by induction on $N$.

(1) Suppose that $f_k = g_k \neq 0$. Since $\alpha$ is right-cancellative $f_0 \cdots f_{k-1} \sim_\alpha g_0 \cdots g_{k-1}$ and by induction hypothesis $f_0 \cdots f_{k-1} \sim_{R_a} g_0 \cdots g_{k-1}$; hence $f \sim_{R_a} g$.

(2) Suppose that $f_k > g_k$. We know that $g_k = f_k - 1$, $g_{k-1} = a$. We obtain that $f_0 \cdots f_{k-1} 1 \sim_\alpha g_0 \cdots g_{k-2} a 0$. If $f_k > 1$, by induction hypothesis, $f_0 \cdots f_{k-1} 1 \sim_{R_a} g_0 \cdots g_{k-2} a 0$, and by Lemma 7, $f \sim_{R_a} g$.

If $f_k = 1$, then $g_k = 0$, $g_{k-1} = a$, and $f_{k-1} = 0$ (Lemma 5). So $f_0 \cdots f_{k-2} 01 \sim_\alpha g_0 \cdots g_{k-2} a 0$.

($\alpha$) If $f_{k-2} \leqslant a - b$, we obtain that $g_0 \cdots g_{k-2} a 0 \sim_\alpha f_0 \cdots (f_{k-2} + b)\, a 0$, i.e., $g_0 \cdots g_{k-2} \sim_\alpha f_0 \cdots (f_{k-2} + b)$ since $\alpha$ is right-cancellative. So $g_0 \cdots g_{k-2} \sim_{R_a} f_0 \cdots (f_{k-2} + b)$; thus $g = g_0 \cdots g_{k-2} a 0 \sim_{R_a} f_0 \cdots (f_{k-2} + b)\, a 0 \sim_{R_a} f$.

($\beta$) If $f_{k-2} > a - b$, we know by Lemma 6 that $f_{k-2} = a - b + 1$ and $g_{k-2} = a$. So $f_0 \cdots f_{k-3} 1 \sim_\alpha g_0 \cdots g_{k-3} 0$ and by induction hypothesis, $f_0 \cdots f_{k-3} 1 \sim_{R_a} g_0 \cdots g_{k-3} 0$. By Lemma 7, $f_0 \cdots f_{k-3}(a - b + 1) \sim_{R_a} g_0 \cdots g_{k-3}(a - b)$, and $f = f_0 \cdots f_{k-3}(a - b + 1)\, 01 \sim_{R_a} g_0 \cdots g_{k-3}(a - b)\, 01 \sim_{R_a} g$. ∎

We now consider the rewriting system on $[s]^*$, where $s \geqslant a$, derived from the rule $ba0 \to 001$, that is the rewriting system $\rho_s = \{h(a+j)k \to (h-b)j(k+1) \mid b \leqslant h \leqslant s,\ 0 \leqslant k \leqslant s-1,\ 0 \leqslant j \leqslant s-a\}$. In this system, any right side is greater for the ordering $\succ$ than the corresponding left side.

The case where $s = a$ is by far the most interesting one.

We use terminology and results of [9].

Lemma 8. *If $s = a$, $\rho_s$ is confluent. If $s > a$, $\rho_s$ is not confluent.*

*Proof.* First suppose that $s = a$. We have $\rho_a = \{hak \to (h-b)\, 0(k+1) \mid b \leqslant h \leqslant a,\ 0 \leqslant k \leqslant a-1\}$. We claim that $\rho_a$ is locally confluent. Since $\rho_a$ is noetherian, $\rho_a$ is then confluent.

Let us consider the critical pair $halak$. We can reduce it this way, $halak \to (h-b)\,0(l+1)\,ak \to (h-b)\,0(l+1-b)\,0(k+1)$, or this way, $halak \to ha(l-b)\,0(k+1) \to (h-b)\,0(l-b+1)\,0(k+1)$, and we obtain the same irreducible word mod $\rho_a$. Then $\rho_a$ is confluent.

Second, suppose that $s > a$. We consider the word $(a+1)\,aa0$. We first reduce it this way, $(a+1)\,aa0 \to (a+1-b)\,0(a+1)0$, which is irreducible. We can also have $(a+1)\,aa0 \to (a+1)(a-b)\,0(a+1)$, which is also irreducible mod $\rho_s$, but different from the first one. So $\rho_s$ is not confluent when $s > a$. ∎

We then get

COROLLARY 2. *If $s = a$, the congruence generated by $R_a$ on $[a]^*$ is equal to $\rho_a^* \cup (\rho_a^{-1})^*$, where $\rho_a^*$ is the reflexive and transitive closure of $\rho_a$.*

## 5. Normalization in a Perfect System

Recall that the canonical representation of an integer $N$, which we denote by $\langle N \rangle$, is the word which is the greatest for the ordering $\succ$ in the set of words representing $N$. Taking any word $f$ representing an integer $\pi(f)$, the word $\bar{f} = \langle \pi(f) \rangle$ is the normal form of $f$. This defines the normalization function $\nu: f \mapsto \bar{f} = \langle \pi(f) \rangle$.

We are now studying the properties of $\nu$ in the perfect case, that is when $s = a$ and $u = a+1$.

We set $L_a = \{hak \mid b \leqslant h \leqslant a,\ 0 \leqslant k \leqslant a-1\}$ and $M_a = \{(h-b)\,0(k+1) \mid b \leqslant h \leqslant a,\ 0 \leqslant k \leqslant a-1\}$.

Let $K_a$ be the rational language equal to the set $\{f \in [a]^* \mid f$ has no factor in $L_a\}$. We have

PROPOSITION 9. *Every word $f$ of $[a]^*$ is congruent* mod $R_a$ *to a unique word $f'$ of $K_a$, which is irreducible* mod $\rho_a$, *and which is greater than or equal to $f$ for the ordering $\succ$.*

*Proof.* Since $\rho_a$ is confluent, $f'$ is necessarily unique. Every step of the reduction $\rho_a$ replaces a word of $L_a$ by a word of $M_a$ which is greater for $\succ$. ∎

From this result we can define a function called *reduction* and denoted by $\rho^*$, which maps every word $f$ of $[a]^*$ onto the word $\rho^*(f) = f'$.

Given a word $w$ of $[a]^*$ and a set $X \subseteq [a]^*$, $wX^{-1}$ denotes the set $\{u \in [a]^* \mid \exists u' \in X,\ uu' = w\}$.

The normal form of a word $f$ not belonging to $0^*$ is obtained by adding a 0 to the right-hand side of $f$, then by calculating the reduced word

$\rho^*(f0)$, and by removing all the 0's left on the right-hand side of the resulting word, that is,

PROPOSITION 10. *The normal form of a word $f$ of $[a]^*\backslash 0^*$ is*

$$\nu(f) = (\rho^*(f0))(0^*)^{-1} \cap \{0, 1\}^* 1.$$

By convention the normal form of a word of $0^+$ is 0.

We are going to show that the normalization $\nu$ is a rather simple function: it is a rational function, easily obtained from the numeration system $(U_{a+1}, a)$.

To the reduction function $\rho^*$, we associate a left-subsequential function and a right-subsequential function. A subsequential function is a function realized by a subsequential transducer, which is a generalized sequential machine with a final output function. (Formal definitions can be found in Berstel [1].) The left-subsequential function $\gamma$ associated to $\rho^*$ reduces a word $w \bmod \rho_a$ from left to right. $\gamma$ is defined as follows:

- if $x \in [a]$ and $w \in [a]^*$,

$$\begin{aligned} \gamma(wx) &= zv \qquad \text{if} \quad \gamma(w) = zt \text{ and } tx \to v \text{ is in } \rho_a \\ &= \gamma(w)x \text{ else.} \end{aligned}$$

The right-subsequential function $\delta$ does the same thing, but from right to left. We define $\delta$ by

- if $x \in [a]$ and $w \in [a]^*$,

$$\begin{aligned} \delta(xw) &= vz \qquad \text{if} \quad \delta(w) = tz \text{ and } xt \to v \text{ is in } \rho_a \\ &= x\delta(w) \text{ else.} \end{aligned}$$

It is convenient to associate transducers to subsequential functions. $\gamma$ is realized by the following left-subsequential transducer $\Gamma$, which reads words and writes the output from left to right.

- The set of states of $\Gamma$ is the set of strict left factors of $L_a$, i.e., $Q_\Gamma = \{\varepsilon, h, ha \mid b \leqslant h \leqslant a\}$.

- By the Fig. 1, we mean that there is a transition from the state $k$ to the state $k'$ in the underlying deterministic finite automaton by reading a word $x$ and outputting a word $y$.

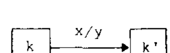


FIGURE 1

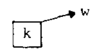


FIGURE 2

– Figure 2 shows that when the reading of a word is finished and we are in state $k$, we concatenate the word $w$ with the word which has been already output.

We summarize the behaviour of $\Gamma$ in Fig. 3, with $b \leqslant h \leqslant a$, $0 \leqslant k \leqslant a-1$, $b \leqslant t \leqslant a-1$, $0 \leqslant l \leqslant b-1$, considering the integer $h$ as a typical state. Similarly, $\delta$ is realized by the right-subsequential transducer $\Delta$, which reads and writes words from right to left. The set of states of $\Delta$ is the set of strict right factors of $L_a$, i.e., $Q_\Delta = \{\varepsilon, k, ak \mid 0 \leqslant k \leqslant a-1\}$.

The rules of $\Delta$ are symbolized in Fig. 4, with $b \leqslant h \leqslant a$, $0 \leqslant k \leqslant a-1$, $0 \leqslant l \leqslant b-1$, $0 \leqslant j \leqslant a-1$, and considering $k$ as a typical state.

EXAMPLE 3 (continued).

$$u_{n+2} = 2u_{n+1} + u_n$$

$$u_0 = 1, \qquad u_1 = 3, \qquad s = 2.$$

We have $\rho_2 = \{120 \to 001,\ 220 \to 101,\ 121 \to 002,\ 221 \to 102\}$. The normal form of the word 2222021 is the word 1020002. The associated transducers are shown in Fig. 5.

We can now state

THEOREM 3. *The reduction $\rho^*$ associated to the perfect system $(U_{a+1}, a)$ is equal to $\gamma \circ \delta$ and to $\delta \circ \gamma$.*

*Proof.* Let $f$ be a word of $[a]^*$. We prove by induction on $|f|$ that $\rho^*(f) = \delta \circ \gamma(f)$.

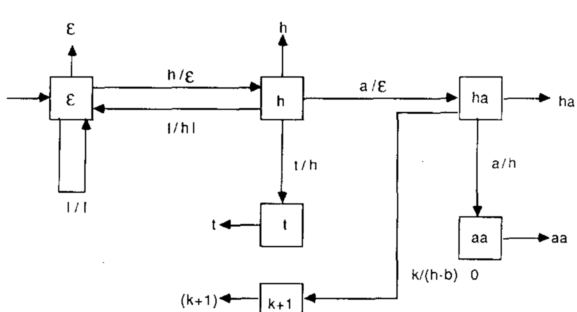


FIGURE 3

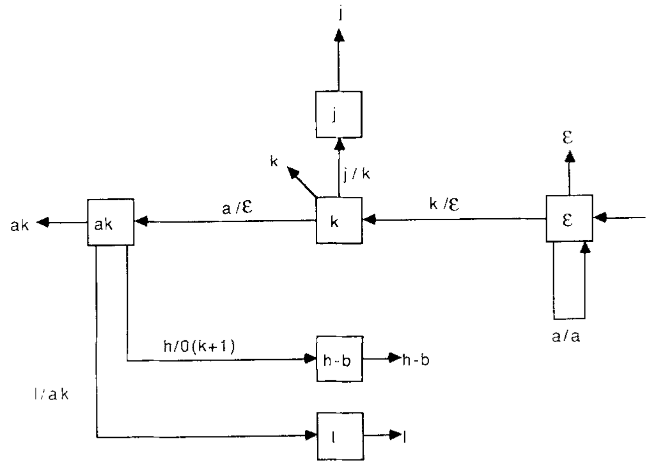


FIGURE 4

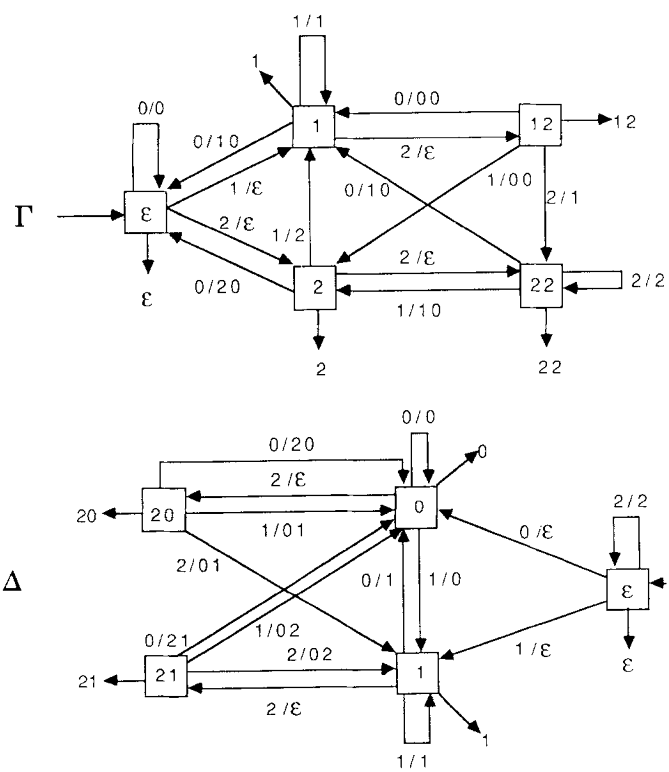


FIGURE 5

1. Let $|f|=3$. If $f$ is reducible mod $\rho_a$, it is because $f=hak$, with $b \leqslant h \leqslant a$, $0 \leqslant k \leqslant a-1$. Then $\gamma(f)=\delta(f)=(h-b)\,0(k+1)=\delta \circ \gamma(f)=\gamma \circ \delta(f)=\rho^*(f)$.

2. Suppose that $|f|>3$. If $\gamma(f)$ is irreducible mod $\rho_a$, then

$$\delta \circ \gamma(f)=\gamma(f)=\rho^*(f).$$

If $\gamma(f)$ is reducible mod $\rho_a$, we can write $f=f_1 hakf_2$, where $f_1 h$ is irreducible. We obtain $\gamma(f)=f_1(h-b)\,0\gamma((k+1)f_2)$, since $\gamma$ is working from left to right. Then, when we apply $\delta$ to $\gamma(f)$, the factor $\gamma((k+1)f_2)$ gives $\delta \circ \gamma((k+1)f_2)$, which is a word having no left factor that can be reduced with a right factor of $f_1(h-b)0$ (the "0" is like a separator). So it is possible to use the induction hypothesis, and we obtain that $\delta \circ \gamma((k+1)f_2)$ is irreducible.

We now consider the factor $f_1(h-b)0$. If it is reducible, $f_1$ is equal to $f'_1xa$, where $b \leqslant x \leqslant a$. But, since $f_1h$ is irreducible by hypothesis, we have necessarily $h=a$. Thus the factor $xa(h-b)=xa(a-b)$ will be reduced in $(x-b)\,0(a-b+1)$, i.e., $\delta(f_1(h-b)0)=\delta(f'_1(x-b))\,0(a-b+1)0$.

As before, $\delta(f'_1(x-b))$ has no right factor which can be reduced with a left factor of $0(a-b+1)0$. So we can use the induction hypothesis, which implies that $\delta(f'_1(x-b))$ is irreducible. So we have that $\delta \circ \gamma(f)=\delta(f'_1(x-b))\,0(a-b+1)\,0\delta \circ \gamma((k+1)f_2)$ is irreducible mod $\rho_a$, i.e., $\delta \circ \gamma(f)=\rho^*(f)$.

That $\gamma \circ \delta=\rho^*$ can be proven in a similar way. ∎

In the case where $a=1$, $b=1$, i.e., the classical Fibonacci system, this result is due to Sakarovitch [12].

*Remarks.* The reduction $\rho^*$ cannot be realized by a single subsequential function. To prove this let us introduce some definitions ([4]). Let $d$ be a distance function on a free monoid $A^*$ and $\varphi$ be a function from $A^*$ to a free monoid $B^*$; $\varphi$ is said to be a *bounded variation function with respect to the distance $d$* if

$$\forall k \geqslant 0, \exists K \geqslant 0, \qquad \text{s.t. } d(x, y) \leqslant k \Rightarrow d(\varphi(x), \varphi(y)) \leqslant K,$$

where $x, y \in A^*$.

It is known from [4] that a left- (resp. right)-subsequential function is a bounded variation function with respect to the left-distance $d_l$ (resp. to the right-distance $d_r$) defined as follows: $d_l(x, y)=|x|+|y|-2|x \wedge_l y|$ where $x \wedge_l y$ denotes the longest prefix common to $x$ and $y$; $d_r(x, y)=|x|+|y|-2|x \wedge_r y|$ where $x \wedge_r y$ denotes the longest suffix common to $x$ and $y$.

Let us now consider the words $x_1 = (aa)^n0$ and $y_1 = (aa)^na0$. We have $\rho^*(x_1) = (a-b)\,0((a-b+1)0)^{n-1}1$ and $\rho^*(y_1) = a(a-b)\,0((a-b+1)0)^{n-1}1$.

Since $d_l(x_1, y_1) = 3$ and $d_l(\rho^*(x_1), \rho^*(y_1)) = 4n+3$, $\rho^*$ is not a bounded variation function with respect to $d_l$ and thus $\rho^*$ cannot be realized by a left-subsequential function.

Similarly, consider $x_2 = ((b-1)a)^n0$ and $y_2 = aa((b-1)a)^n0$. We have $\rho^*(x_2) = x_2 = ((b-1)a)^n0$ and $\rho^*(y_2) = (a-b)\,0(00)^n1$. Thus $d_r(x_2, y_2) = 2$ and $d_r(\rho^*(x_2), \rho^*(y_2)) = 4n+4$, and $\rho^*$ cannot be realized by a right-subsequential function.

COROLLARY 3. *The normalization associated to a perfect system is a rational function.*

*Proof.* Theorem 3 implies that $\rho^*$ is a rational function, and, by Proposition 10, $\nu$ also is rational. ∎

We must link the result of Theorem 3 to the Theorem of Elgot and Mezei which states that every rational function is the product of a left-sequential function by a right-sequential function.

The fact that the reduction here is a rational function is not at all the general rule: to every confluent and noetherian rewriting system one can associate a reduction function. But this function need not be rational, as is shown by the example $xy \to 1$ (cf. [12]).

To a rewriting system, it is possible to associate in a natural way a left- and a right-subsequential function, but in the general case the reduction, even if it is rational, is not equal to the product of these subsequential functions.

EXAMPLE. The rewriting system $xzyzz \to zzyx$ is noetherian and confluent. It can be shown that the associated reduction is a rational function, which is equal to $\delta \circ \gamma \circ \delta$, where $\gamma$ and $\delta$ are the left- and right-subsequential functions associated to the reduction function as in Theorem 3.

## 6. ADDITION IN A PERFECT SYSTEM

The aim of this section is to show that the addition of two integers represented in a perfect numeration system is a rational function. This result is already known for $k$-ary systems [7, 1].

Let $f$ and $g$ be two words of $[a]^*$ respectively representing the integers $N$ and $P$. To make the addition of $N$ and $P$ in the system, we simply add digit by digit, in a parallel manner; i.e., we obtain a word $h = f + g$ on the alphabet [2a].

EXAMPLE 3 (continued).

$$u_{n+2} = 2u_{n+1} + u_n$$

$$u_0 = 1, \qquad u_1 = 3, \qquad s = 2$$

$$\begin{array}{rcccc}
 & 1 & 3 & 7 & 17 \cdots \\
\hline
14 = & 1 & 2 & 1 & \\
21 = & 1 & 2 & 2 & \\
\hline
35 = \begin{cases} \\ \\ \end{cases} \!\!\!\!\!\!\! & \begin{matrix} 2 \\ 1 \end{matrix} & \begin{matrix} 4 \\ 1 \end{matrix} & \begin{matrix} 3 \\ 2 \end{matrix} & \begin{matrix} \\ 1, \end{matrix}
\end{array}$$

$f = 121$, $g = 122 \in [2]^*$. We obtain $h = 243$ on the alphabet $[4]^*$, which is equivalent to the word 1121 on $[2]^*$.

Now, we must transform $h$ into a word $\lambda(h)$ which has the same numerical value as $h$ and which belongs to $[a]^*$. This is a kind of normalization, which will be proved to be performed by a right-subsequential function $\lambda$. Of course, the resulting word $\lambda(h)$ need not be in normal form. To obtain that, it is necessary to apply the normalization function $\nu$ to $\lambda(h)$.

THEOREM 4. *Let $p$ be an integer, $p \geqslant 0$. There exists a right-subsequential function $\lambda_p$: $[a+p+1]^* \to [a+p]^*$ such that $\lambda_p(h)$ and $h$ have the same numerical value.*

COROLLARY 4. *The addition of two integers in a perfect system is right-subsequential.*

*Proof.* The parallel addition digit by digit is obviously subsequential. The resulting word $h$ belongs to $[2a]^*$. The successive applications of the functions $\lambda_{a-1}, \lambda_{a-2}, \ldots, \lambda_0$ to $h$ give a word $\lambda(h)$ belonging to $[a]^*$, i.e.,

$$\lambda(h) = \lambda_0 \circ \lambda_1 \circ \cdots \circ \lambda_{a-1}(h).$$

Since the composition of right-subsequential functions is again right-subsequential, the addition is right-subsequential. ∎

*Proof of Theorem 4.* We have the two fundamental equivalences

$$ba0 \sim_\alpha 001$$

$$00(a+1)0 \sim_\alpha b(a-b)\,01.$$

From these equivalences, we define the rewriting systems $S_p$:

$$S_p \begin{cases} (1) & h(a+p+i)k \to (h-b)(p+i)(k+1) \\ (2) & zx(a+p+j)k \to (z+b)(x+a-b)(p+j-1)(k+1) \\ & \text{with } b \leqslant h \leqslant a+p+1, 0 \leqslant i \leqslant b+1, \\ & 0 \leqslant k \leqslant a+p-1, 0 \leqslant x \leqslant b-1, \\ & 1 \leqslant j \leqslant b+1, 0 \leqslant z \leqslant a+p+1. \end{cases}$$

The rules (1) consist only in the reduction $\rho$ on the extended alphabet $[a+p+b+1]$ (the necessity for considering such an alphabet will be explained infra). When the reduction $\rho$, that is rules (1), is not possible, and this is the case when $a+p+j$ is preceded by a digit $x$ less than $b$, we use rules (2). These two sets of rules clearly do not change the numerical value of words.

We must now distinguish three cases according to the value of $a$ and $b$.

*Case* 1. $b \geqslant 2$. As in the preceding section, to the rewriting system $S_p$ we associate a right-subsequential transducer $A_p$ which performs $S_p$ from right to left.

The set of states $Q_p$ is the set of strict right factors of left members of $S_p$, i.e.,

$$Q_p = \{k \mid 0 \leqslant k \leqslant a+p-1\} \cup \{(a+p+i)k \mid 0 \leqslant i \leqslant b+1, \\ 0 \leqslant k \leqslant a+p-1\} \cup \{x(a+p+j)0 \mid 0 \leqslant x \leqslant b-1, \\ 1 \leqslant j \leqslant b+1, 0 \leqslant k \leqslant a+p-1\}.$$

The initial state is 0.

For transitions and output, see Fig. 6.

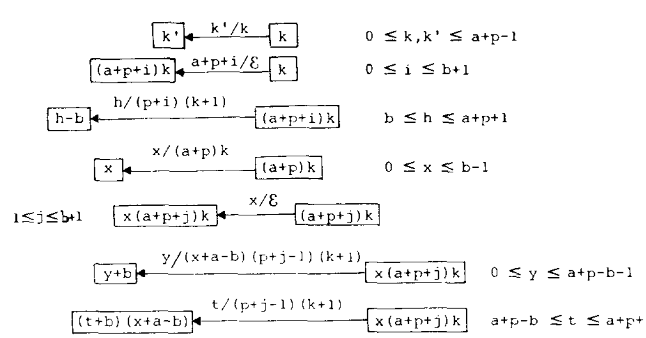


FIGURE 6

$$\boxed{h-b} \xleftarrow{h/(p+1+b)(x+a-b+1)} \boxed{(a+p+1+b)(x+a-b)}$$

FIGURE 7

The final output function $\omega$ associated to every state is defined by

$$\omega(k)=k$$
$$\omega((a+p)k)=(a+p)k$$
$$\omega((a+p+j)k)=(p+j-1)(k+1)$$
$$\omega(x(a+p+j)k)=(x+a-b+1)(p+j-1)(k+1).$$

It is necessary to consider the extended alphabet $[a+p+b+1]$ because the word $(a+p+1)\,0(a+p+1)0$ gives $(a+p+b+1)(a-b)\,p1$ when it is reduced by $S_p$ (2).

When a word[2] belonging to $[a+p+1]^*$ is processed by $\Lambda_p$ the resulting word belong to $[a+p]^*$ unless $a=b$. Hence we consider two cases

(a) $a>b$. We thus have, if $w\in[a+p+1]^*$, $\Lambda_p(w)\in[a+p]^*$, and $\pi(w)=\pi(\Lambda_p(w))$.

(b) $a=b$. The only problem is the transition (see Fig. 7) since, if $a=b$, a letter $a+p+1$ will be output. The solution is to process the resulting word $\Lambda_p(w)$ once more in $\Lambda_p$. We must examine why we are in such a situation. This is because we have a factor $h(a+p+1)x(a+p+1)k$ in $w$, with $a\leqslant h\leqslant a+p-1$, $0\leqslant x\leqslant a-1$, $0\leqslant k\leqslant a+p-1$ (see Fig. 8).

The corresponding output factor is $(a+p+1)(x+1)\,p(k+1)$, which does not make any problem when it is processed once more by $\Lambda_p$, because the state $(2a+p+1)x$ is never reached. Then, if $w\in[a+p+1]^*$ and $a=b$, $\Lambda_p^2(w)\in[a+p]^*$ and $\pi(w)=\pi(\Lambda_p^2(w))$.

*Case* 2. $b=1$, $a\geqslant 2$. We must modify the transducer $\Lambda_p$ since, if $h=a+p+1$, $h-b=a+p$ cannot be a state of $Q_p$. We define a right-subsequential transducer $\Sigma_p$, much like $\Lambda_p$, but we must introduce two special states which allow the reading of words "in advance." The alphabet is $[a+p+1]^*$.

We take, as a set of states, $S_p=\{k\mid 0\leqslant k\leqslant a+p-1\}\cup\{(a+p+i)k\mid 0\leqslant k\leqslant a+p-1,\ 0\leqslant i\leqslant 1\}\cup\{0(a+p+1)k\mid 0\leqslant k\leqslant a+p-1\}\cup\{s_1,s_2\}$ where $s_1$ and $s_2$ are two special states. The initial state is 0.

Transitions and output are shown in Fig. 9. $s_1$ is like $1(a-1)\cdot p0(p+1)$, which $1(a-1)$ read in advance, and $s_2$ is $1\cdot(a-1)p$ with 1 read in

[2] As in Proposition 10, we must add a 0 to the right-hand side of a word before reading it.

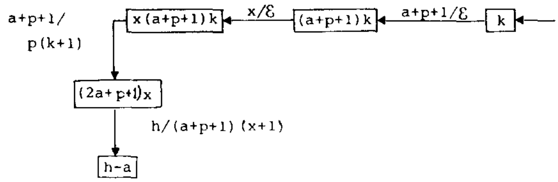


FIGURE 8

advance. The final output function $\omega$ is defined as in Case 1, with $\omega(s_1) = p0(p+1)$ and $\omega(s_2) = ap$. The output word belongs to $[a+p]^*$.

*Case* 3. Fibonacci: $a = b = 1$. The transducer $\Sigma_p$ does not work, because $(a+p)(p+1)$ is not allowed as a state $(p+1 > a+p-1 = p)$. We define on $[p+2]^*$ a right-subsequential transducer $\mathscr{T}_p$, derived from $\Sigma_p$. The set of states is $T_p = \{k \mid 0 \leqslant k \leqslant p\} \cup \{(p+1)k \mid 0 \leqslant k \leqslant p\} \cup \{(p+2)k \mid 0 \leqslant k \leqslant p\} \cup \{0(p+2)k \mid 0 \leqslant k \leqslant p\} \cup \{s_0, s_1, s_2\}$ where $s_0 = (p+1)(p+1)$ is a special state, $s_1$ and $s_2$ are as in $\Sigma_p$ (see Fig. 10).

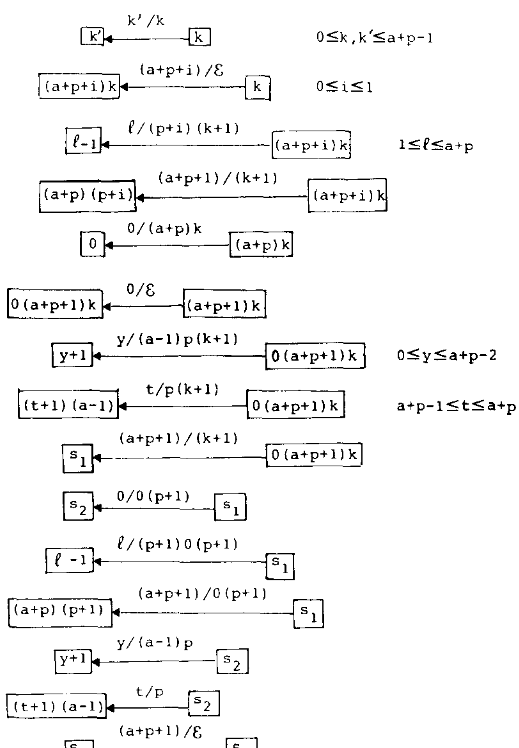


FIGURE 9

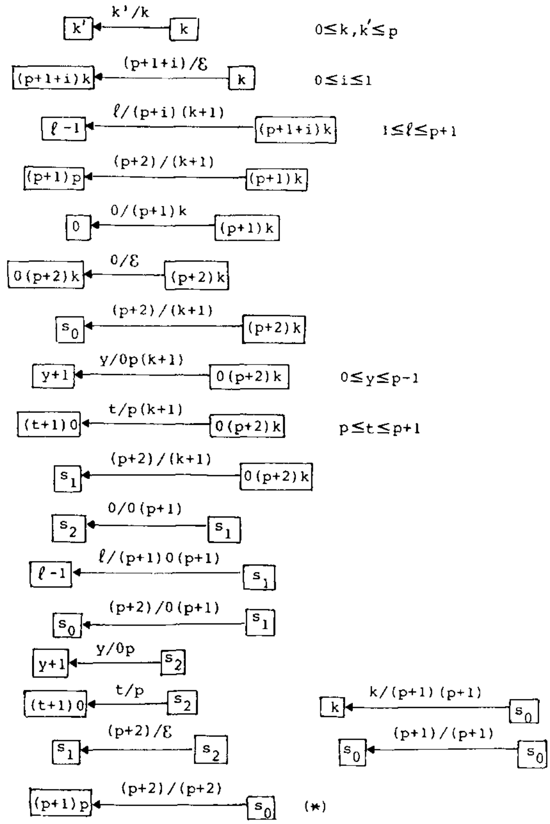


FIGURE 10

We have $\omega(s_0)=(p+1)(p+1)$, $\omega(s_1)=p0(p+1)$, and $\omega(s_2)=1p$. The output word belongs to $[p+1]^*$ except when transition (*) is used. As in Case 1, we use $\mathscr{T}_p$ twice. When we input a word having a factor $l(p+2)^n(p+2)(p+1)^m(p+2)(p+2)k$, where $m, n \geqslant 0$, $0 \leqslant k \leqslant p$, $1 \leqslant l \leqslant p+2$, the image factor is $(l-1)\,p(p+1)(p+1)^n(p+2)(p+1)^m(k+1)$, which when processed one more time in $\mathscr{T}_p$ does not reach the state $s_0$. If we consider the factor $0(p+2)^n(p+1)(p+1)^m(p+2)(p+2)k$, the image is $0(p+1)\,p(p+1)^n(p+2)(p+1)^m(k+1)$ and we have finished. Since we process words belonging to $[p+2]^*0$, the result after two applications of $\mathscr{T}_p$ belongs to $[p+1]^*$.

For the Fibonacci case, Berstel has given a right-subsequential transducer which transforms in one time words of $[2]^*$ into words of $[1]^*$ (Ref. [2]). ∎

*Remarks.* (1) The addition cannot be realized by a left-subsequential function. Consider the words on $[2a]^*$ $w=0(0a)^n 0(2a)0$ and $y=0(0a)^n 0a0$. The equivalent words on $[a]^*$ are $w'=b(a-b)((b-1)(a-b+1))^n(a-1)1$ and $y'=y$. Since $d_l(w, y)=4$ and $d_l(w', y')=4n+8$, the addition is not a left-bounded variation function and so cannot be realized by a left-subsequential function (cf. Section 5).

(2) It is noteworthy that, on the contrary, in a $k$-ary system the addition is left-subsequential [6, 1]. It cannot be realized by a right-subsequential function, as is shown by this example. In the binary system, consider $w=21^n0$ and $y=1^{n+1}0$ on $\{0, 1, 2\}^*$. The equivalent words on $\{0, 1\}^*$ are $w'=0^{n+1}1$ and $y'=y$. We have $d_r(w, y)=2$ and $d_r(w', y')=2n+4$.

(3) As we have shown in Proposition 5, the system defined by

$$\begin{aligned} u_{n+2} &= au_{n+1}+(a+1)u_n \\ u_0=1, &\qquad u_1=a+1 \end{aligned} \tag{1}$$

with alphabet $\{0, ..., a\}$ reduces to the classical $(a+1)$-ary system. If we try to formally apply the techniques of Theorem 4 to (1), we see that no word containing the digit $(a+1)$ can be written on the alphabet $[a]$ (compare wiith $00(a+1)0 \sim_\alpha b(a-b)\,01$ in Theorem 4). So there is really a difference between $k$-ary systems and systems of order two.

We now consider linear numeration systems defined by the same equation $u_{n+2}=au_{n+1}+bu_n$, $u_0=1$, $u_1=a+1$, $a \geqslant b$, with a finite arbitrary set of digits $D$. We have

PROPOSITION 11. *There exists a right-subsequential function which transforms every word on $D^*$ into a word on $[a]^*$ which has the same numerical value.*

*Proof.* $D$ can be embedded into a set $\{0,..., t\}$. If $t \leqslant a$, there is nothing to do. If $t > a$, $t$ is equal to $a+p+1$ for some $p \geqslant 0$. By Theorem 4 we are done. ∎

So it is always possible to reduce to the perfect case in a subsequential manner.

ACKNOWLEDGMENT

I thank the anonymous referee for his helpful remarks and suggestions.

RECEIVED October 23, 1986; ACCEPTED November 16, 1987

## References


1. Berstel, J. (1979), "Transductions and Context-Free Languages," Teubner, Stuttgart.
2. Berstel, J. (1986), Fibonacci words—A survey, "The Book of $L$," pp. 13–27, Springer-Verlag, Berlin/New York.
3. Carlitz, L. (1968), Fibonacci representations, *Fibonacci Quart.* **6**(4), 193–220.
4. Choffrut, Ch. (1977), Une caractérisation des fonctions séquentielles et des fonctions sous-séquentielles en tant que relations rationnelles, *Theoret. Comput. Sci.*, **5**, 325–337.
5. Culik, K., II, and Salomaa, A. (1983), Ambiguity and decision problems concerning number systems, "Lecture Notes in Computer Science Vol. 154," pp. 137–146, Springer-Verlag, Berlin/New York.
6. Eilenberg, S. (1974), "Automata, Languages and Machines," Vol. A, Academic Press, New York.
7. Fraenkel, A. S. (1985), Systems of numeration, *Amer. Math. Monthly* **92**(2), 105–114.
8. Honkala, J. (1984), Bases and ambiguity of number systems, *Theoret. Comput. Sci.* **31**, 61–71.
9. Huet, G. (1980), Confluent reductions: Abstract properties and applications to term rewriting systems, *J. Assoc. Comput. Mach.* **27**, 797–821.
10. Knuth, D. E. (1975), "The Art of Computer Programming," Vols. 1, 2, and 3, Addison-Wesley, Reading, MA.
11. de Luca, A., and Restivo, A. (1984), Representations of integers and language theory, "Lecture Notes in Computer Science Vol. 176," pp. 407–415, Springer-Verlag, Berlin/New York.
12. Sakarovitch, J. (1987), Easy multiplications, *Inform. and Comput.* **74**(3), 173–197.
13. Zeckendorf, E. (1972), Representation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas, *Bull. Soc. Roy. Sci. Liège* **3–4**, 179–182.